Technical Cybersecurity

Theft & Extortion

Ransomware, Botnets, Carding, Credentials, Extortion

Ransomware

Targets

- Commercial and Consumer

Infection Vectors

- Botnets, worms, trojans

Remediation

- Flaw in crypto system, adequate backup strategy

Botnets

Targets

- All the things (workstations, servers, IoT, mobile)

Infection Vectors

- Worms, trojans (and PUPs, potentially unwanted programs), phishing

Remediation

- Can sometimes be manually removed, Anti-malware

Carding

Targets

- Corporate retail, PoS

Infection Vectors

- Sophisticated, external hacking ops, spearphishing, social engineering

Remediation

- Backups, custom analysis, reinstallation, replace cards

Credentials

Targets

- Corporate, internet companies, information companies

Infection Vectors

- External hacking, phishing

Remediation

- Repair infected systems, change credentials

Extortion

Targets

- Individuals

Infection Vectors

- Phishing, hacking, social engineering

Remediation

- Don’t do things you can be extorted with :-(

Intel ops!